

Amendments to the Claims

Claims 1-18 (Canceled)

Claim 19 (New) A playback terminal for playing back content, the playback terminal comprising:

a content read unit operable to read encrypted content from a portable medium, the encrypted content being data generated by encrypting the content so that one of (a) medium information pre-stored on the portable medium and (b) rights information managed by an external license server is required for decrypting the encrypted content, the rights information including usage rights for the content;

a decryption method judgment unit operable to judge whether or not the rights information is required for decrypting the encrypted content;

a medium information read unit operable to read the medium information from the portable medium;

a rights information acquisition unit operable to acquire the rights information from the external license server; and

a decryption unit operable to decrypt the encrypted content using the medium information and without using the rights information when it is judged that the rights information is not required, and decrypt the encrypted content using the rights information when it is judged that the rights information is required.

Claim 20 (New) The playback terminal of claim 19, wherein

the medium information includes a media key, and

the decryption unit includes:

a content key obtaining sub-unit operable to, when it is judged that the rights information is not required, obtain the media key from the medium information and, using the obtained media key, obtain a first content key used in decrypting of the encrypted content; and

a content decryption sub-unit operable to, when it is judged that the rights information is not required, decrypt the encrypted content using the first content key.

Claim 21 (New) The playback terminal of claim 20, wherein

the content key obtaining sub-unit, when it is judged that the rights information is required, obtains a second content key used in decrypting of the encrypted content, using the rights information, and

the content decryption sub-unit, when it is judged that the rights information is required, decrypts the encrypted content using the second content key.

Claim 22 (New) The playback terminal of claim 21, wherein

the rights information includes a rights key, and

the content key obtaining sub-unit, when it is judged that the rights information is required, obtains the second content key using the rights key.

Claim 23 (New) The playback terminal of claim 22, wherein

the content key obtaining sub-unit, when it is judged that the rights information is required, obtains the second content key using both the rights key and the media key.

Claim 24 (New) The playback terminal of claim 21, wherein

the portable medium further has stored thereon key obtaining information indicating whether or not the rights information is required for obtaining a key used for decrypting the encrypted content, and

the playback terminal further comprises:

a key obtaining information read unit operable to read the key obtaining information from the portable medium, wherein

the decryption method judgment unit performs the judgment of whether or not the rights information is required for decrypting the encrypted content, based on the key obtaining information.

Claim 25 (New) The playback terminal of claim 20, wherein

the decryption unit, when it is judged that the rights information is necessary, performs decryption of the encrypted content only when the rights information acquisition unit has already

acquired the rights information and the rights information indicates that usage of the content is permitted.

Claim 26 (New) The playback terminal of claim 20, further comprising:

a holding unit operable to hold device unique information that is unique to the playback terminal, wherein

the media key is in an encrypted state, having been encrypted using the device unique information, and

the content obtaining unit, when it is judged that the rights information is not required, obtains the media key by decrypting the encrypted-state media key using the device unique information.

Claim 27 (New) The playback terminal of claim 20, wherein

the portable medium further has stored thereon information indicating whether or not the rights information is required for decrypting of the encrypted content, and

the playback terminal further comprises:

an information read unit operable to read the information from the portable medium, wherein

the decryption method judgment unit performs the judgment of whether or not the rights information is required for decrypting the encrypted content, based on the information.

Claim 28 (New) A content playback method used in a playback terminal for playing back content, the content playback method comprising:

reading encrypted content from a portable medium, the encrypted content being data generated by encrypting the content so that one of (a) medium information pre-stored on the portable medium and (b) rights information managed by an external license server is required for decrypting the encrypted content, the rights information including usage rights for the content;

judging whether or not the rights information is required for decrypting the encrypted content;

reading the medium information from the portable medium;

acquiring the rights information from the external license server; and

a decryption step of decrypting the encrypted content using the medium information and without using the rights information when it is judged that the rights information is not required, and decrypting the encrypted content using the rights information when it is judged that the rights information is required.

Claim 29 (New) The content playback method of claim 28, wherein

the medium information includes a media key, and

the decryption step includes:

a content key obtaining sub-step of, when it is judged that the rights information is not required, obtaining the media key from the medium information and, using the obtained media key, obtaining a first content key used in decrypting of the encrypted content; and

a content decryption sub-step of, when it is judged that the rights information is not required, decrypting the encrypted content using the first content key.

Claim 30 (New) The content playback method of claim 29, wherein

the content key obtaining sub-step includes, when it is judged that the rights information is required, obtaining a second content key used in decrypting of the encrypted content, using the rights information, and

the content decryption sub-step includes, when it is judged that the rights information is required, decrypting the encrypted content using the second content key.

Claim 31 (New) The content playback method of claim 30, wherein

the rights information includes a rights key, and

the content key obtaining sub-step includes, when it is judged that the rights information is required, obtaining the second content key using the rights key.

Claim 32 (New) The content playback method of claim 31, wherein

the content key obtaining sub-step includes, when it is judged that the rights information is required, obtaining the second content key using both the rights key and the media key.

Claim 33 (New) The content playback method of claim 30, wherein

the portable medium further has stored thereon key obtaining information indicating whether or not the rights information is required for obtaining a key used for decrypting the encrypted content, and

the content playback method further comprises:

reading the key obtaining information from the portable medium, wherein

the judging comprises judging whether or not the rights information is required for decrypting the encrypted content, based on the key obtaining information.

Claim 34 (New) The content playback method of claim 29, wherein

the decryption step includes, when it is judged that the rights information is necessary, performing decryption of the encrypted content only when the acquiring has already acquired the rights information and the rights information indicates that usage of the content is permitted.

Claim 35 (New) The content playback method of claim 29, wherein

the playback terminal includes a holding unit operable to hold device unique information that is unique to the playback terminal,

the media key is in an encrypted state, having been encrypted using the device unique information, and

the content key obtaining sub-step includes, when it is judged that the rights information is not required, obtaining the media key by decrypting the encrypted-state media key using the device unique information.

Claim 36 (New) The content playback method of claim 29, wherein

the portable medium further has stored thereon information indicating whether or not the rights information is required for decrypting of the encrypted content, and the content playback method further comprises:

reading the information from the portable medium, wherein

the judging comprises judging whether or not the rights information is required for decrypting the encrypted content, based on the information.

Claim 37 (New) A portable recording medium having storing thereon
medium information,

encrypted content that is data generated by encrypting the content so that one of (a) the
medium information and (b) rights information managed by an external license server is required
for decrypting the encrypted content, and

information indicating whether or not the rights information is required for decrypting the
encrypted content.